UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,310	07/03/2001	Teng Pin Poo	1601457-0008	2223

7590 08/24/2005

White and Case LLP
Attn: Patent Department
1155 Avenue of the Americas
New York, NY 10036

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2133	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/898,310	POO ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/28/05,5/31/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on May 19, 2005. Claims 1, 3-5, 11, 13-14, 17, 20-21 have been amended. Claims 1-21 are pending.

Claim Objections

2. In view of Applicant's amendment, the previous objection to claim 9 is withdrawn.

Claim Rejections - 35 USC § 101

3. In view of the terminal disclaimer filed on May 19, 2005, the Examiner withdraws the double patenting rejection of claims 1-21.

Response to Arguments

4. Applicant's arguments see Remarks, filed May 19, 2005, with respect to the rejection(s) of claim(s) 1-21 have been considered but are not persuasive. In response to the arguments concerning the previously rejected claims, the following comments are made:

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a portable device that can be directly plugged into a USB socket communicatively coupled to a restricted resource and which has a USB plug integrated into its housing without an intervening cable and capable of coupling the device directly to the USB socket, or the use of such a device in an access control system) are not recited in the

rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Applicant argues Bialick does not teach or suggest a bypass mechanism. The Examiner disagrees although Bialick does not explicitly disclose bypass mechanism; he teaches the device can be implemented in order to enable the user to enter an acceptable access code such as password or PIN before allowing access. (Col. 10, lines 45-47) It would have been obvious to use the password or PIN to allow access in case of failure of the biometric-based authentication, because as suggested by Bialick the system can be set up in order to authenticate the user using biometric or password or PIN to have a layer of security that protects the integrity of the restricted resources.

The Applicant argues Bialick does not teach a device that can provide access control to a communication network. The Examiner strongly disagrees. Bialick teaches the peripheral device can be made accessible to the host computing device via an appropriate interface such as network connection. (Col. 9; lines 9-11) It is well known in the art a network connection is setup in order to have a network communication. Therefore, it would have been obvious to modify Bialick's method to include the restricted resource comprises a communication network.

The Applicant argues Bialick does not teach or suggest encrypting and storing the biometrics marker. The Examiner disagrees although Bialick does not explicitly disclose encrypting the biometrics marker, he teaches encrypting and decrypting data

stored on the host-computing device. (Col. 12, lines 12-13) It would have been obvious to encrypt and store the biometrics marker in order to protect the biometric data from being compromised. Furthermore, it is well known in the art to store passwords and other authentication information in an encrypted format.

Regarding claims 3 and 13, the Applicant argues Bjorn does not teach or disclose a universal serial bus (USB) connector for coupling with another USB-compliant device. Bjorn teaches a device with a digital connection, a bus that conforms to a universal serial bus (USB). (Col. 2, lines 59-60). Bjorn further the USB is used to receive digitized image that is another USB-compliant device. Therefore, Bjorn clearly anticipates the claimed USB connector for coupling another USB-compliant device.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both Bialick and Burger are directed toward using biometric authentication in order to access a restricted resource. It would have been obvious to modify the system disclosed by Bialick in order to provide an open, stand-alone system which protects the real estate premises by enforcing proper biometric authentication as suggested by Burger (Col. 3, lines 46-47).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1-8 and 11-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. (hereinafter Bialick) United States Letters Patent No. 6,088,802 in view of Estakhri et al. (hereinafter Estakhri) United States Letters Patent No. 6,385,667. As per claim 1:

Bialick et al. teach a unitary portable biometric-based access control device comprising:

housing; (Figure 3a)

a microprocessor housed within the housing; and (Figure 8, item 801)

a biometrics-based authentication module coupled to and controlled by the microprocessor (Col. 5; lines 1-2; the peripheral device also provides the capability to accept biometric input to enable user authentication to the host computing device), at least a portion of the biometrics-based authentication module being housed within the housing, wherein access to the restricted is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise. (Col. 14; lines 50-52; biometric user authentication to a host computing device is made before allowing access to particular data stored on the host computing device.)

In addition, Bialick discloses a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket.

Estakhri in analogous art, however, teaches a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket. (Figure 3, element 300, element 314, element 335, element 330; Col. 5, lines 19-51)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick to include a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket. This

modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Estakhri, (Col. 1, lines 16-17) in order to provide an interface facilitating user-friendly connectivity and a faster transfer of digitized image.

As per claim 2:

The rejection of claim 1 is incorporated and further Bialick discloses the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28; a sensor for sensing the fingerprint of the finger, the content of the sensed fingerprint being converted into digital data by the device.)

As per claim 3:

The rejection of claim 1 is incorporated and further Bialick discloses a device wherein the biometrics-based authentication module is an iris scan authentication module. (Col. 14, lines 29-33)

As per claim 4:

The rejection of claim 1 is incorporated and further Bialick discloses the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the housing. (Col. 14, lines 48-49; a peripheral device includes a biometric device which includes a sensor for sensing the fingerprint)

As per claim 5:

The rejection of claim 1 is incorporated and further Bialick discloses a non-volatile memory capable of storing biometrics information usable for authentication. (Figure 8, item 803; Col. 16; lines 10-11; the first memory device can be a non-volatile

data storage device which can be used to store computer programs and persistent data.)

As per claim 6:

The rejection of claim 1 is incorporated and further Bialick discloses the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick is that, the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick's method to include a microprocessor that is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

As per claim 7:

The rejection of claim 1 is incorporated and further Bialick discloses the restricted resource comprises a host computer. (Col. 14; lines 50-51; to enable user authentication to a host computing device.)

As per claim 8:

The rejection of claim 1 is incorporated and further Bialick discloses the peripheral device can be made accessible to the host computing device via an appropriate interface such as network connection. (Col. 9; lines 9-11) Not explicitly disclosed by Bialick is that, the restricted resource comprises a communication network. However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick's method to include the restricted resource comprises a communication network. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to use the security functionality of host computing device to a communication network.

As per claim 11:

Bialick et al. teach a biometrics-based access control system for controlling access to a restricted resource, comprising:

housing; (Figure 3a) a non-volatile memory housed within the housing; (Figure 8, item 803) and a biometrics-based authentication module coupled to the non-volatile memory, wherein the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (Col. 14, lines 55-56; an appropriate library of biometric data representing a predetermined group of people; which indicates obtaining the biometrics of authorized users the first time) (2) store the first biometrics marker in the non-volatile memory; (Col. 14; lines 57-58; the library data can be stored in a memory device of the peripheral device) (3) capture a second biometrics marker; (Col.14; line 54; obtain biometric data from a user) and (4) determine whether the

second biometrics marker can be authenticated against the first biometrics marker, and wherein access to the restricted resource is granted upon a determination of successful authentication and wherein access to the restricted resource is denied otherwise. (Col. 14; lines 50-52; biometric user authentication to a host computing device is made before allowing access to particular data stored on the host computing device.)

In addition, Bialick discloses a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource and which includes a housing; and a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device to the USB socket.

Estakhri in analogous art, however, teaches a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource and which includes a housing; (Figure 3, element 300, element 314) and a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device to the USB socket. (Figure 3, element 300, element 314, element 335, element 330; Col. 5, lines 19-51)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick to include a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource and which includes a housing; and a USB plug integrated into the housing without an intervening cable and capable of

coupling the portable device to the USB socket. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Estakhri, (Col. 1, lines 16-17) in order to provide an interface facilitating user-friendly connectivity and a faster transfer of digitized image.

As per claim 12:

The rejection of claim 11 is incorporated and further Bialick discloses the biometrics-based authentication module is a fingerprint authentication module. (Col. 14, lines 26-28; a sensor for sensing the fingerprint of the finger, the content of the sensed fingerprint being converted into digital data by the device.)

As per claim 13:

The rejection of claim 11 is incorporated and further Bialick discloses a device wherein the biometrics-based authentication module is an iris scan authentication module. (Col. 14, lines 29-33)

As per claim 14:

The rejection of claim 11 is incorporated and further Bialick discloses the biometrics-based authentication module comprises a biometrics sensor which is structurally integrated with the portable device in a unitary construction, the biometrics sensor being disposed on one surface of the housing of the portable device. (Col. 14, lines 48-49; a peripheral device includes a biometric device which includes a sensor for sensing the fingerprint)

As per claim 15:

The rejection of claim 11 is incorporated and further Bialick discloses the non-volatile memory of the portable device comprises flash memory. (Figure 8, item 803)

As per claim 16:

The rejection of claim 11 is incorporated and further Bialick discloses the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick is that, a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick's method to include a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

As per claim 17:

Bialick teaches a biometrics-based access control method for controlling access to a restricted resource and implemented using a portable device, includes a housing; (Figure 3a) a memory; (Figure 8, item 803) a biometric sensor; and the method comprising the steps of: (b) obtaining a first biometrics marker from a user with the biometrics sensor of the portable device; (Col.14; line 54; obtain biometric data from a

user) (c) retrieving a registered biometrics marker from the memory of the portable device, the registered biometrics marker having been stored therein during a registration process; (Col. 14; lines 57-58; the library data can be stored in a memory device of the peripheral device; the stored biometrics has to be retrieved in order to compare it with the newly obtained biometrics) (d) comparing the first biometrics marker against the registered biometrics marker; (Col. 14; lines 54-56; comparing the biometric data to an appropriate library of biometric data representing a predetermined group of people.) and (e) granting the user access to the restricted resource provided that a match is identified in said step (c). (Col. 14; lines 50-52; biometric user authentication to a host computing device is made before allowing access to particular data stored on the host computing device.)

In addition, Bialick discloses a communication interfaces, such as a smart card interface, a serial interface or a SCSI interface or an IDE interface. Not explicitly disclosed by Bialick (a) directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted resource; (Figure 3, element 300, element 314) and a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device to the USB socket. (Figure 3, element 300, element 314, element 335, element 330; Col. 5, lines 19-51)

Estakhri in analogous art, however, teaches directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted resource; (Figure 3, element 300, element 314) and a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device to the

USB socket. (Figure 3, element 300, element 314, element 335, element 330; Col. 5, lines 19-51)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Bialick to include directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted resource; and a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device to the USB socket. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Estakhri, (Col. 1, lines 16-17) in order to provide an interface facilitating user-friendly connectivity and a faster transfer of digitized image.

As per claim 18:

The rejection of claim 17 is incorporated and further Bialick discloses biometrics-based access control method as recited in claim 17 wherein the registered biometrics marker is a fingerprint. (Col. 14, lines 26-28; a sensor for sensing the fingerprint of the finger, the content of the sensed fingerprint being converted into digital data by the device.)

As per claim 19:

The rejection of claim 17 is incorporated and further Bialick discloses the peripheral device can be used to encrypt or decrypt data stored. Not explicitly disclosed by Bialick is that, the registered biometrics marker is stored in an encrypted format.

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick's method to include the registered biometrics marker is stored in an encrypted format. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to enhance the security of the biometrics-based access control method.

As per claim 20:

The rejection of claim 17 is incorporated and further Bialick discloses the step of denying the user access to the restricted resource provided that a match is not identified in said step (d). (Col. 14; lines 50-52; biometric user authentication to a host computing device is made before allowing access to particular data stored on the host computing device. the user authentication is made in order to grant or deny access to the host computer depending the result of the comparison)

As per claim 21:

The rejection of claim 17 is incorporated and further Bialick discloses the peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. (Col. 10; lines 45-47) Not explicitly disclosed by Bialick is that, providing the user with a bypass authentication procedure provided that a match is not identified in said step (d).

However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Bialick's method to include providing the

user with a bypass authentication procedure provided that a match is not identified in said step (c). This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources.

7. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. United States Letters Patent No. 6,088,802 and in view of Burger United States Letters Patent No. 6,219,439.

As per claim 9:

Bialick et al. teach all the subject matter as described above. In addition, Bialick et al. disclose the restricted resource comprises a host computer. Not explicitly disclosed by Bialick et al. is the restricted resource is a real estate premises that imposes access restrictions.

Burger in analogous art, however, teaches the restricted resource is a real estate premises that imposes access restrictions. (Figure 2; Col. 6; lines 39-40; a user attempts to gain access through the door by inserting their card into the reader so that the stored template of their fingerprint can be read.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Burger to include the restricted resource is a real estate premises that imposes access restrictions. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Burger, (Col. 3; line 38) in order

to provide an open, stand-alone system which protects the real estate premises by enforcing proper biometric authentication.

As per claim 10:

Bialick et al. teach all the subject matter as described above. In addition, Bialick et al. disclose the restricted resource comprises a host computer. Not explicitly disclosed by Bialick et al. is the restricted resource is an operable machinery, the safe operation of which requires training.

Burger in analogous art, however, teaches the restricted resource is an operable machinery, the safe operation of which requires training. (Col. 8; lines 27-28; the system can be mounted to the dashboard to control use of the steering wheel.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Burger to include the restricted resource is an operable machinery, the safe operation of which requires training. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Burger, (Col. 3; line 38) in order to provide an open, stand-alone system which protects the machinery by enforcing proper biometric authentication.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay SG
08/19/05